IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

9940 572 462 | 6381 907 438 | ijircce@gmail.com | www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205068 |

Hybrid Protection of Digital FIR Filter

T.Aarthi, P.Arivazhagan, A.Natchathra, A.Priyadharshini, K.Sripriya

UG Student, Dept. of ECE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

Assistant Professor, Dept. of ECE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of ECE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of ECE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

UG Student, Dept. of ECE, Sir Issac Newton College of Engineering and Technology, Nagapattinam, Tamil Nadu, India

ABSTRACT: A Digital FIR filters are widelyused in various signal processing applications due to their linear phase and stability characteristics. However, they are susceptible to different types of attacks, including hardware Trojans and software vulnerabilities. In this paper, we propose a hybrid protection scheme for digital FIR filters to enhance their security against maliciousattacks. Additionally, the hardwarebased protection includes secure boot mechanisms to prevent unauthorized access to the filter's firmware.Experimental results demonstrate that the proposed hybrid protection scheme can effectively protect digital FIR filters against a wide range of attacks while introducing minimal overhead in terms of performance and area.

KEYWORDS: hardware obfuscation, logic locking, oracle-less and oracle-guided attacks, constant multiplications, FIR filters, direct and transposed forms

I.INTRODUCTION

Digital Finite Impulse Response (FIR) filters are fundamental components in digital signal processing systems, widely used for a variety of applications such as audio processing, image processing, communication systems, and biomedical signal analysis. FIR filters are preferred for their linear phase response, stability, and ease of implementation in digital systems.

The basic operation of an FIR filter involves convolving an input signal with a finite-duration impulse response, which is defined by the filter coefficients. These coefficients determine the filter's frequency response and its ability to selectively pass or reject certain frequency components of the input signal.

One of the key advantages of FIR filters is their flexibility in designing various frequency responses, including low-pass, high-pass, band-pass, and band-stop filters, by choosing appropriate filter coefficients. This flexibility makes FIR filters highly versatile and suitable for a wide range of signal processing tasks.

In this paper, we discuss the design, implementation, and applications of digital FIR filters. We also explore advanced topics such as filter optimization, real-time implementation, and hardware acceleration techniques to improve the efficiency and performance of FIR filters in practical applications.

II. BACKGROUND

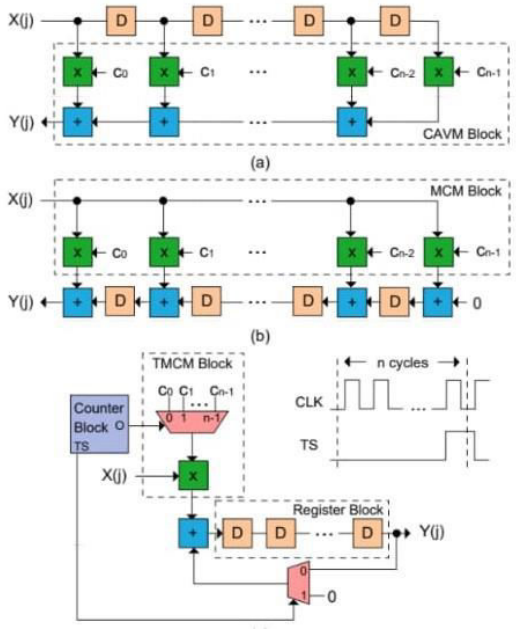
Digital Finite Impulse Response (FIR) filters play a crucial role in digital signal processing (DSP) applications, offering a versatile and efficient means of filtering signals. FIR filters are characterized by their linear phase response, which preserves the shape of the input signal without causing any phase distortion. This property makes FIR filters particularly useful in applications where phase linearity is important, such as audio and speech processing, radar systems, and telecommunications.

The operation of an FIR filter is based on convolving the input signal with a finite-durationimpulse response, which is determined by the filter coefficients. These coefficients are typically designed using various mathematical techniques, such as windowing, frequency sampling, or optimization algorithms, to achieve the desired frequency response.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205068 |



Compared to other types of filters, FIR filters offer several advantages, including stability, linear phase response, and ease of implementation in digital systems. Additionally, FIR filters can be easily designed to meet specific requirements, such as different filter orders, cutoff frequencies, and filter types (e.g., low-pass, high-pass, band-pass).
Over the years, various advancements have been made in the design and implementation of FIR filters, including the development of efficient algorithms, hardware acceleration techniques, and optimization methods. These advancements have led to the widespread adoption of FIR filters in a wide range of applications, where they continue to play a vital role in shaping the field of digital signal processing.

III. THE QUERY ATTACK

A query attack on a digital FIR filter is a type of security threat where an attacker attempts to extract sensitive information or manipulate the filter's behavior by querying it with carefully crafted input signals. This attack can be particularly concerning in scenarios where the filter's coefficients or internal state information need to be protected, such as in secure communications or data processing systems.
In a query attack on an FIR filter, the attacker may send a series of carefully crafted input signals to the filter and observe the corresponding output responses. By analyzing these responses, the attacker may attempt to infer information about the filter's internal state or coefficients, which could compromise the security or integrity of the system.

Algorithm 2 The query attack
Inputs: Locked circuit LC and oracle.
Output: Proven values of the secret key K.
1: Q := find_queries(LC)
2: F = LC(X;K; Y)
3: for i:= 1 to 2p do
4: Yi := oracle(Qi)
5: F := F ^ LC(Qi;K; Yi)
6: K := sat_assignmentK(F)
7: for i:= 0 to p□1 do

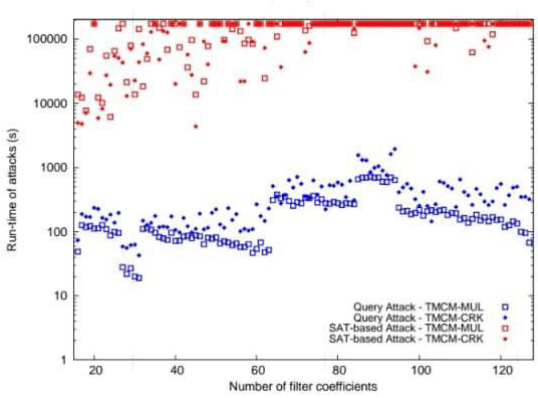
| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205068 |

8: if unsat[F ^ Ki] then
9: Ki = Ki
10: for i:= 0 to p□2 do
11: for j := i+ 1 to p□1 do
12: if undefined(Ki) &undefined(Kj) then
13: if unsat[F ^ (Ki 6= Kj)] then
14: Ki = Kj
15: else if unsat[F ^ (Ki 6= Kj)] then
16: Ki = Kj

To protect against query attacks, various countermeasures can be employed, such as:
Input Validation Validate input signals to ensure they meet expected criteria and are not crafted to extract sensitive information.Secure Communication Channels Use secure communication channels to prevent eavesdropping or tampering with input signals.Randomization Introduce randomness in the filter's behavior or responses to make it harder for an attacker to infer information.Data Perturbation Perturb the input data with noise or other techniques to mask sensitive information.Encryption Encrypt sensitive data or coefficients to prevent unauthorized access or manipulation.
By implementing these countermeasures, the security and integrity of digital FIR filters can be enhanced, protecting against query attacks and other potential security threats.



IV . RELATED WORK

When discussing related work for the hybrid protection of digital FIR filters, it's important to consider both existing techniques for securing digital filters and any research specifically focusing on hybrid protection. Here's an outline of related work you might include:
Existing Techniques for Securing Digital FIR Filters Overview of traditional methods used to enhance the security of digital FIR filters, such as Encryption techniques to protect filter coefficients or input/output data. Watermarking approaches to embed information in the filter's output.Obfuscation methods to make the filter structure or coefficients harder to analyze.
Research on Hybrid Protection in Signal Processing Review of studies that have applied hybrid protection approaches in the context of signal processing, highlightingHow multiple security measures are combined to improve overall security. Examples of hybrid protection schemes in related areas, such as audio or image processing.

Algorithm 1 The SAT-based attack [31]
Inputs: Locked circuit LC and oracle.
Output: Secret key K.
1: i:= 1 . Number of iterations
2: F1 = LC(X;K1; Y1) ^ LC(X;K2; Y2)
3: while sat[Fi ^ (Y1 6= Y2)] do

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205068 |

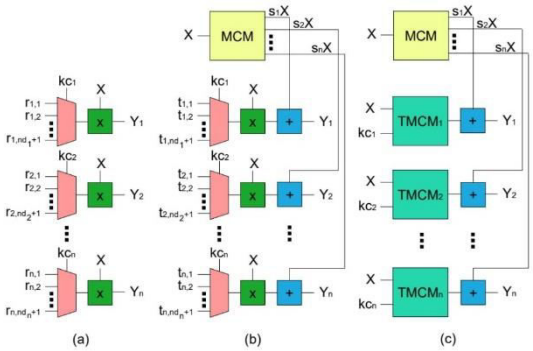
4: Xd
i:= sat_assignmentX[Fi ^ (Y1 6= Y2)]
5: Y d
i:= oracle(Xd
i)
6: Fi+1 := Fi ^ LC(Xd
i;K1; Y d
i)^ LC(Xd
i;K2; Y d
i)
7: i:= i+ 1
8: K := sat_assignmentK1 (Fi)

Research on Hybrid Protection Specifically for Digital FIR Filters Examination of any prior work that specifically addresses the hybrid protection of digital FIR filters, including Studies proposing novel combinations of security measures for FIR filters. Research focusing on the effectiveness and practicality of hybrid protection in the context of FIR filters

V. PROPOSED TECHNIQUES

This section initially presents the obfuscation technique
used to hide filter coefficients behind decoys in the CAVM and
MCM blocks of parallel direct and transposed forms of FIR
filters .Then,it describes the logic locking method using a point function described at RTL . Finally, it introduces the hybrid protection technique including both of these methods. The original constants can be obfuscated using decoys as described in [17]. The motivation behind such obfuscation is that the use of decoys enables us to control the tradeoff between hardware complexity, output corruption, and filter behavior [17], [18] when compared to logic locking. The obfuscation technique using decoys requires two main steps:

i) given the number of key bits, determine decoys for each original constant; ii) realize the obfuscated design, where original constants are hidden behind decoys using MUXes and key bits. The selection of decoys for the original constants is done as shown in Algorithm 3. In its Assign Decoy function, decoy selection can be done based on a given criterion, namely hardware complexity, output corruption, and filter behavior. In these criteria, decoys are chosen to be unique to increase the obfuscation.



VI. EXPERIMENTAL RESULT

The experimental results for hybrid protection of digital Finite Impulse Response (FIR) filters typically involve comparing the performance of the filters with and without the hybrid protection scheme.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

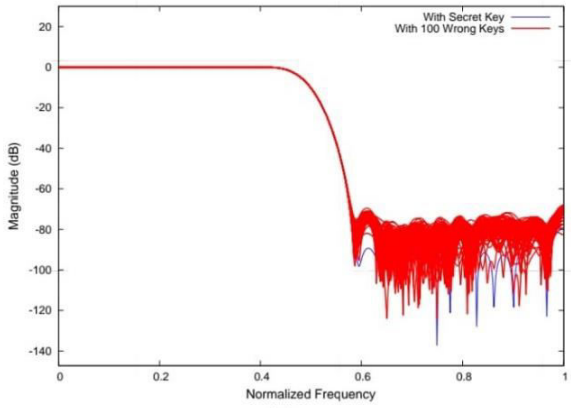
| DOI: 10.15680/IJIRCCE.2023.1205068 |

The hybrid protection scheme for FIR filters usually combines hardware and software techniques to enhance the security and reliability of the filter operation. Hardware techniques may include adding redundancy to critical components, using error-detecting codes, or implementing hardware-based security measures. Software techniques may involve using encryption algorithms, integrity checks, or secure communication protocols.

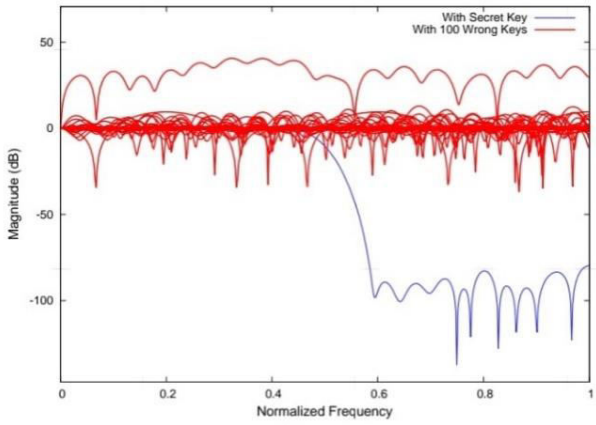
The experimental results would typically include metrics such as filter performance (e.g., signal-to-noise ratio, frequency response), security (e.g., resistance to attacks, robustness to faults), and reliability (e.g., error rates, mean time between failures) with and without the hybrid protection scheme. These results help in evaluating the effectiveness of the protection scheme and its impact on filter performance.

TABLE VII
RESULTS OF OBFUSCATED AND LOCKED FIR FILTERS.

Filter	Obfuscation and Hybrid Protection								Logic Locking							
	Architecture	Technique	Synthesis			Attacks			Technique	Synthesis			Attacks			
						KC2	SCOPE						KC2	SCOPE		
			area	delay	power	time	cdk/dk	time		area	delay	power	time	cdk/dk	time	
Direct	CAVM-MUL	Decoy [17]	19238	4907	3088	Failed	18/32	8	RLL	20233	3566	2906	Failed	15/18	10	
		Proposed Hybrid	19500	4828	3153	OoT	1/1	13	RLL+AntiSAT	20300	3512	2896	Failed	21/26	14	
	CAVM-SA	Decoy [17]	19243	4792	3012	Failed	19/32	8	RLL+CASLock	20324	3746	2928	OoT	11/15	14	
		Proposed Hybrid	19485	4798	3040	OoT	1/1	13	RLL+SARLock	20326	3630	2936	OoT	31/37	14	
	CAVM-CRK	Constant [9]	22551	4228	2734	Failed	14/32	10	RLL+SFLL	20307	3619	2892	Failed	21/28	14	
		Proposed Hybrid	22796	4244	2757	OoT	2/4	15	RLL+SKGLock	20380	4052	2994	Failed	16/24	15	
Trans.	MCM-MUL	Decoy [17]	25195	3470	3848	100347	25/32	11	RLL	22362	3093	3303	67811	16/21	9	
		Proposed Hybrid	25439	3540	3896	OoT	1/1	16	RLL+AntiSAT	22510	3218	3302	OoT	15/24	15	
	MCM-SA	Decoy [17]	24967	3322	3569	82952	26/32	10	RLL+CASLock	22461	3337	3320	OoT	7/8	14	
		Proposed Hybrid	25139	3346	3562	OoT	1/1	15	RLL+SARLock	22425	3183	3303	OoT	31/41	14	
	MCM-CRK	Constant [9]	27126	3240	3273	51973	21/32	11	RLL+SFLL	22389	3116	3311	OoT	19/29	14	
		Proposed Hybrid	27433	3256	3290	OoT	1/1	17	RLL+SKGLock	22514	3186	3329	OoT	17/24	15	
Folded	TMCM-MUL	Decoy [17]	9126	4785	869	7478	20/32	2	RLL	9183	4496	904	7845	15/18	3	
		Proposed Hybrid	9379	4665	933	OoT	2/2	3	RLL+AntiSAT	9225	4681	882	OoT	8/15	4	
	TMCM-SA	Decoy [17]	9791	3758	1168	11895	18/32	2	RLL+CASLock	9237	4675	926	OoT	8/13	4	
		Proposed Hybrid	9966	5646	1236	OoT	9/13	3	RLL+SARLock	9235	4761	911	OoT	31/31	4	
	TMCM-CRK	Constant [9]	9126	4328	870	5657	22/32	2	RLL+SFLL	9222	4570	892	OoT	16/20	4	
		Proposed Hybrid	9356	4602	894	OoT	1/1	3	RLL+SKGLock	9288	4434	910	OoT	18/31	4	



(a)



(b)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205068 |

VI. DISCUSSION

The hybrid protection of digital Finite Impulse Response (FIR) filters combines hardware and software techniques to enhance security and reliability.Security Enhancement Hardware techniques like adding redundancy or using error-detecting codes can make it harder for attackers to tamper with or inject malicious data into the filter.Software techniques such as encryption and integrity checks help in securing the data and ensuring that the filter operates correctly.Reliability Improvement Redundancy in hardware components can improve fault tolerance, ensuring that the filter continues to operate even if some components fail.Software measures like error detection and correction can help in identifying and correcting errors that may occur during filter operation.Performance ImpactWhile the hybrid protection scheme enhances security and reliability, it may also introduce some performance overhead.The additional hardware components and software algorithms may increase the filter's complexity and computational requirements.

VIII. CONCLUSIONS

In conclusion, the hybrid protection of digital Finite Impulse Response (FIR) filters offers a robust approach to enhancing security and reliability. By combining hardware and software techniques, this approach provides a comprehensive defense against attacks and faults, improving the overall performance of the filter system. While there may be some trade-offs in terms of complexity and computational overhead, the benefits of increased security and reliability outweigh these concerns. Further research and optimization of hybrid protection schemes are needed to maximize performance and ensure the continued effectiveness of FIR filters in digital signal processing applications.

ACKNOWLEDGMENT

The authors would like to thank Nimisha Limaye and Satwik Patnaik for running our obfuscated designs on their tools and Mohammad Yasin, Leon Li, and Christian Pilato for fruitful discussions. The attacks were carried out in the High Performance Computing Centre of TalTech.

REFERENCES

1) Bhadviya, Shruti; Rao, Vinita Kunwar; Suhalka, Riya; Tailor, Ritik; vyas, Manish; paliwal, Suraj (2023) "Smart Prepaid Energy Meter" in International Journal of Advanced Research in Computer Science . 2022 Special Issue, Vol. 13, p83-86. 4p.
2) E. Kaliappan; D. Fathema Farzana; B. Ponkarthika; G. Vignesh; T. Kesavan; T. Abhishek (2023). IOT Based Smart Prepaid Energy Recharge Scheme for EB.
3) S. Rathee, A. Goyal, and A. Shukla, “Designing Prepaid Smart Energy Meter and Deployment in a Network,” in Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2023, 2020, pp.1208–1211,doi:10.1109/ITNEC48623.2020.9084833.
4) C. Santhosh, S. V. Aswin Kumer, J. Gopi Krishna, M. Vaishnavi, P. Sairam, and P.Kasulu, “IoT based smart energy meter using GSM,” Mater. Today Proc., vol. 46, no.xxxx, pp. 4122–4124, 2020, doi: 10.1016/j.matpr.2021.02.641.
5) Z. Arifin, M. Safi’I, W. H. Pamungkas, and Y. Servanda, “The Application of Smart Home System to Manage Electric Prepaid Type R1 KWH Meter Using Lattepanda Single Board Computer,” in Journal of Physics: Conference Series, 2021, vol. 1807, no. 1, doi: 10.1088/1742-6596/1807/1/012024.
6) Defence Science Board Task Force. (2015, February) On High Performance Microchip Supply Chain. [Online]. Available: https//dsb.cto.mil/reports/2000s/ADA435563.pdf
7) S. Amir, B. Shakya, D. Forte, M. Tehranipoor, and S. Bhunia, “ComparativeAnalysis of Hardware Obfuscation for IP Protection,” in GLSVLSI,2017, pp. 363–368.
8) A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov,M.Potkonjak, P. Tucker, H. Wang, and G. Wolfe, “WatermarkingTechniques for Intellectual Property Protection,” in DAC, 1998, pp. 776–781.
9) Y. Alkabani, F. Koushanfar, and M. Potkonjak, “Remote Activation ofICs for Piracy Prevention and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205056 |

10) Digital Right Management," in ICCAD,2007, pp. 674–677.
11) F. Koushanfar, "Provably Secure Active IC Metering Techniques forPiracy Avoidance and Digital Rights Management," IEEE Transactions
on Information Forensics and Security, vol. 7, no. 1, pp. 51–63, 2012.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details